KINA BANK LIMITED

ECOMMERCE MERCHANT INTEGRATION GUIDE

Version 2.3

Document Information

Prepared By	**:** Kina Bank Limited	**Document Version No**	**:** 2.2
		Document Version Date	**:** 09 Sep 2022

Version History

Ver. No.	Ver. Date	Revised By	Remarks
1.0	23 Jun 2020	Tan Kah Hoe	
1.1	24 Jun 2020	Tan Kah Hoe	Switch term ”checkout page” to ”order confimation page” Add section for MAC Calculation
1.2	29 Jun 2020	Tan Kah Hoe	Reshuffle MAC source string order Secret Key for HMAC Testing in TEST environment
1.3	30 Jun 2020	Tan Kah Hoe	List of Action Code in Response List of EGW Response Code (RC)
1.4	07 May 2021	Tan Kah Hoe	Check Transaction request and response
1.5	14 May 2021	Tan Kah Hoe	Include Merchant Test Data (test card, terminal)
1.6	28 Jul 2021	Tan Kah Hoe	Hosted payment page, Embedded payment page Digital Signature for response
1.7	06 Sep 2021	Tan Kah Hoe	Subdomain name change – https://ipg.kinabank.com.pg/
1.8	14 Apr 2022	Tan Kah Hoe	Check Transaction request and response in JSON format Online HMAC calculator
1.9	09 May 2022	Tan Kah Hoe	Switch order, make Embedded Payment Page precede Hosted Payment Page Add JS example code for calculating Hmac
2.0	02 Jun 2022	Tan Kah Hoe	Digital signature in response: outline formattting rules to amount field (2 decimal point)
2.1	22 Jun 2022	Tan Kah Hoe	Bank Transfer - JS function to submit form - New RC -95, -96, -97, -98 - Update Transaction Flows, Digital Signatures, Test Data - Add bank transfer iframe screenshot under embedded payment page
2.2	09 Sep 2022	Tan Kah Hoe	Check transaction - Content-Type = application/json; **charset=utf-8**
2.3	02 Aug 2023	Tan Kah Hoe	Remove Payment by Bank Transfer Remove Check Transaction Request and Response Add TID=99999004 under Test Data
2.4	19 Mar 2023	Tan Kah Hoe	Change domain name: devegateway to test-ipg

Table of Contents

Introduction 3
Transaction Flows 3
Authorization Request 5
Authorization Response 6
Reversal Request 7
Reversal Response 7
Payment Page Integration 8
Embedded Payment Page (iframe) integration guide 9
Hosted Payment Page (redirect) integration guide 10
Digital Signature 11
Secret key 11
MAC source string 11
Digital Signature in Request 12
Digital Signature in Response 13
EGW Response Code 14
Test Data 15
Online HMAC Calculator 16

Introduction

This document illustrates the steps to integrate merchant e-commerce site to Kina Payment Gateway. Kina Payment Gateway support the acceptance of the following Card brands:

1. Visa
2. MasterCard
3. Union Pay
4. Kina Debit Card
5. ANZ Debit Card
6. Mibank Debit Card

Transaction Flows

1. **Checkout Page**
   After selecting good and services, customer proceed to checkout page to fill in delivery info.

2. **Order confirmation page**.
   Upon finalizing delivery info, customer click a button and merchant site display order confirmation page and present payment methods to customer. Order confirmation page must include a HTTP FORM element that contains INPUT or HIDDEN fields (complete set of fields described in next section) required to authorize the transaction, submit HTML FORM to the Kina Payment page URL (described in the integration guide)

3. **Kina Payment Page (Hosted by Kinabank)**
   Depending on the chosen payment method, customer will see different payment page.

   Pay by credit/debit card: a page to collect card details and subsequently autheticate the cardholders with the issuing bank.

   Pay by bank transfer: Kinabank customer can login with their Internet banking credential and then select the account to perform the payment.

4. **Customer click pay**
   In Kina Payment Page iframe, customer fill in card number and other card details, and click pay. Kina payment gateway receive the authorization request and validates request information including the message authentication code (MAC). If the request fails, gateway sends an error response back to merchant system.

5. **Cardholder authentication**.
   If the provided card number belongs to a card range with a defined cardholder authentication method, gateway calls the corresponding authentication module like 3-D Secure, which performs protocol-specific processing like One Time Password. If cardholder authentication is unsuccessful, Gateway returns an error message to the merchant system.

6. **Transaction authorization**

Gateway sends an authorization request to Kina card system. Upon authorization, reception gateway prepares and sends a transaction response back to the merchant system. If authorization is successful, the response message will contain “Internal Reference Number” field, to be used by the merchant system so it can reverse/refund the obtained authorization without the credit card information.

Authorization Request

Following fields set will be posted to Kina Payment Gateway through HTTP POST method. These fields can be rendered as HTML INPUT or HIDDEN elements in order confirmation page. Merchant site should perform basic prevalidation to ensure the values conform to the below requirements

Field	Size	Description
AMOUNT	1-12	Order amount in float format with decimal point separator, up to 2 decimal point. Example: **98.30**
CURRENCY	03	Order currency: 3-character currency code
ORDER	6-20	Merchant order ID, numeric. Last 6 digits used as a system trace audit number, which must be unique within a day for the terminal id.
DESC	1-50	Order description
MERCH_NAME	1-50	Merchant name (recognizable by cardholder)
MERCH_URL	1-250	Merchant primary web site URL
MERCHANT	15	Merchant ID assigned by bank
TERMINAL	8	Merchant Terminal ID assigned by bank
EMAIL	80	E-mail address for notification. If this field is present Gateway may send transaction results notification to specified e-mail address
TRTYPE	2	Must be equal to "1" (Retail Financial Request).
COUNTRY	02	Merchant shop 2-character country code. Must be provided if merchant system located in a country other than the gateway server's country.
MERCH_GMT	1-5	Merchant UTC/GMT time zone offset (e.g. –3). Must be provided if merchant system located in a time zone other than the gateway server's time zone.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between merchant server and e-Gateway server must not exceed 1 hour, otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
BACKREF	1-250	Merchant URL for posting authorization result.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Authorization Response

Kina Payment Gateway processes the authorization request and returns the response to merchant URL provided in the **BACKREF** incoming field. Additionally, the same field set may be sent to the merchant via to the email address provided in the **EMAIL** incoming field.

Field	Size	Description
TERMINAL	8	Echo from the request
TRTYPE	2	Echo from the request
ORDER	6-20	Echo from the request
AMOUNT	12	Amount authorized. Usually, will be equal to original amount plus acquirer fee.
CURRENCY	3	Echo from the request
ACTION	1	E-Gateway action code: 0 – Transaction successfully completed; 1 – Duplicate transaction detected; 2 – Transaction declined; 3 – Transaction processing fault; 4 – Information message.
RC	02	Transaction response code (ISO-8583 Field 39)
APPROVAL	06	Client bank's approval code (ISO-8583 Field 38). Can be empty if not provided by card management system.
RRN	12	Merchant bank's retrieval reference number (ISO-8583 Field 37).
INT_REF	1-32	E-Commerce gateway internal reference number
TIMESTAMP	14	E-Commerce gateway timestamp in GMT: YYYYMMDDHHMMSS
NONCE	1-64	E-Commerce gateway nonce value. Will be filled with 8-32 unpredictable random bytes in hexadecimal format. Will be present if MAC is used.
P_SIGN	1-256	E-Commerce gateway MAC (Message Authentication Code) in hexadecimal form. Will be present if MAC is used.

Reversal Request

The reversal transaction request shall be sent by the merchant system Kina Payment Gateway to cancel previously authorized or completed transactions.

All fields are provided by merchant system and the cardholder does not participate in this transaction.

Field	Size	Description
ORDER	6-20	Merchant order ID from request.
AMOUNT	12	Transaction amount. Float format with decimal point separator.
CURRENCY	3	Currency name. Must be the same as in authorization response.
RRN	12	Retrieval reference number from authorization response.
INT_REF	1-32	Internal reference number from authorization response.
TRTYPE	2	Must be equal to "24" (Reversal Request).
TERMINAL	8	Merchant terminal ID assigned by bank. Must be equal to "TERMINAL" field from authorization request.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between Internet shop and e-Gateway must not exceed 1 hour otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Reversal Response

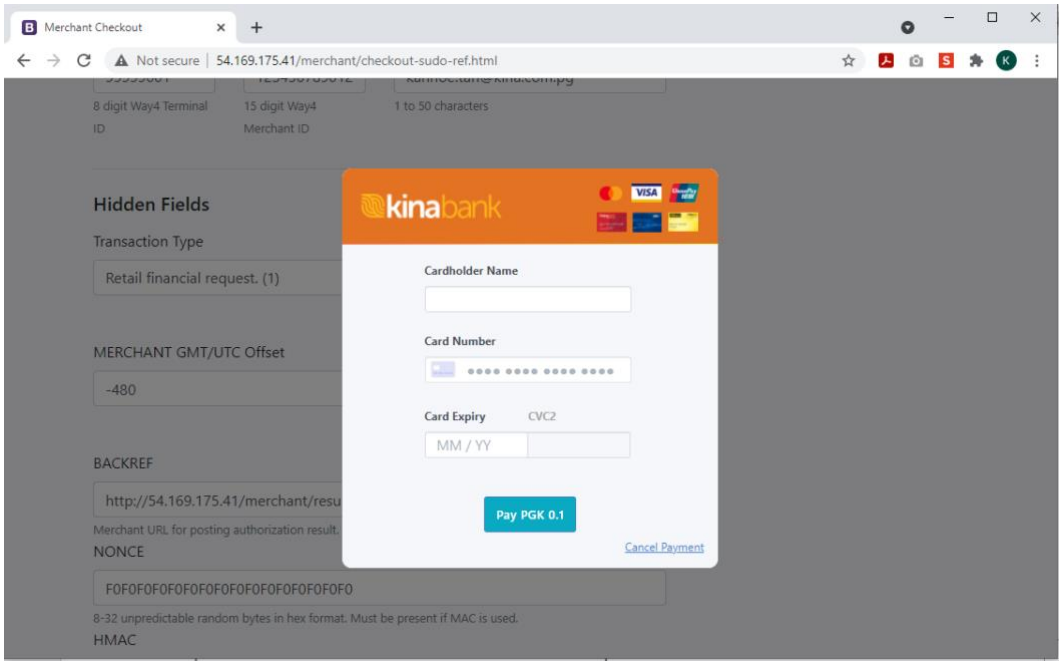
Gateway processes a reversal request and returns the result fields to the merchant system within a response document. Response fields and format are the same as for the authorization response.

Payment Page Integration

Kinabank supports 2 types of payment page.

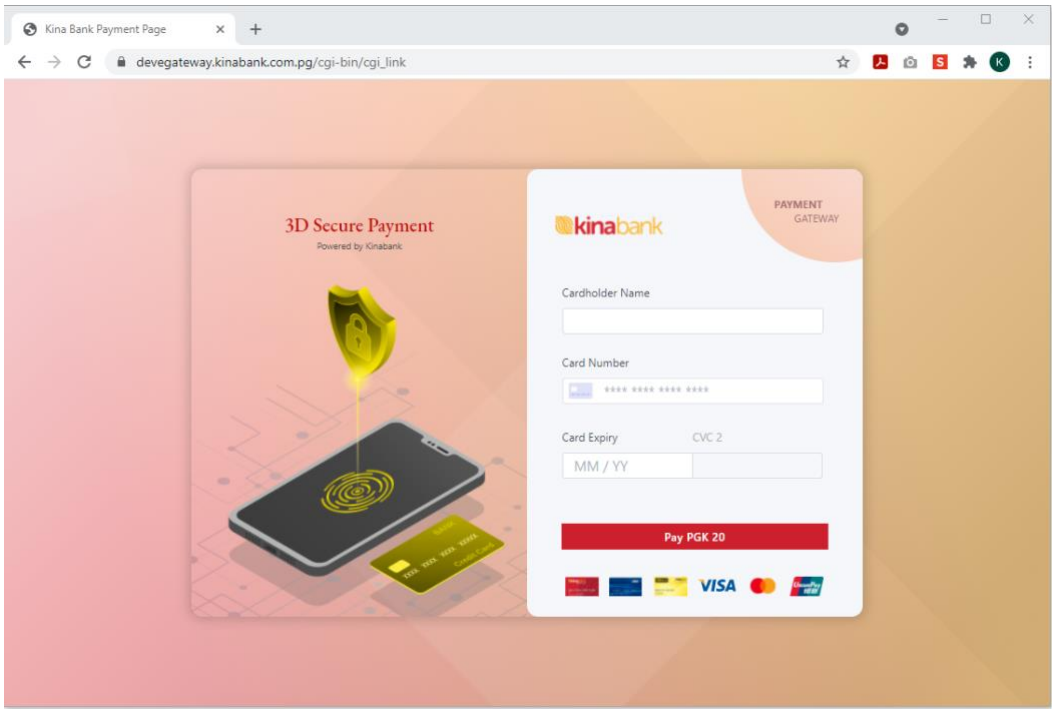
Embedded Payment Page a.k.a. iframe displays the payment form as overlay, consumer stays on the merchant site rather than being redirected to a separate site.

iframe – Pay by card



Hosted Payment Page redirect the consumer to a standalone payment page hosted by Kinabank.

Hosted Payment Page – Pay by Card



Embedded Payment Page (iframe) integration guide

In the <head> of order confirmation page

```
<head>
  <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
  <meta http-equiv="Pragma" content="no-cache" />
  <meta http-equiv="Expires" content="0" />
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <script src="https://test-ipg.kinabank.com.pg/kina/js/kbl-ec.js"></script>
  <link href="https://test-ipg.kinabank.com.pg/kina/css/kbl-ec.css" rel="stylesheet">
</head>
```

*In Production, substitute `https://test-ipg.kinabank.com.pg` with `https://ipg.kinabank.com.pg`

Cache-Control, Pragma and Expires meta tag ensure the page and its content are not cached, use of these meta elements are strongly recommeded, these directive will ensure the browser to fetch a fresh copy of the page resources (CSS, JS and Images) from the server rather than using the cache version, which may be outdated.

Viewport meta tag, it's recommeded to use this tag for fluid and responsive design that looks good in both desktop and mobile

kbl-ec.js and **kbl-ec.css** are mandatory javascript and css to support the functions and the look and feel of the payment page, its recommended to append some random number like timestamp to prevent caching, example: `kbl-ec.js?202109061545123`

In the <body> of order confirmation page

```
<body>
  <form id="kblPaymentForm" method="POST" target="kblpaymentiframe">
    <input type="text"…/>
    <input type="hidden"…/>
    …
    …
  </form>

  <button type="button" onclick="submitPaymentForm2()">Pay by Cards</button>
  <button type="button" onclick="submitPaymentForm2('bank-transfer')">Bank Transfer</button>

  <div id="kbliframediv" class="kbliframeoverlay">
    <div id="kbliframeinnerdiv">
       <iframe id="kblpaymentiframe" name="kblpaymentiframe"></iframe>
    </div>
  </div>

</body>
```

<Form> tag enclose all INPUT fields described in Authorization Request, it's advisable to disable editing for all input fields (or using hidden fields) and MAC is precalculated in the P_SIGN fields.

To invoke **"payment by card"**, call javascript function **submitPaymentForm2()**, this will make the iframe visible and submit the HTML forms to iframe. Before calling this function, please ensure all INPUT/HIDDEN fields and their values conform to the requirements stated in this manual.

Hosted Payment Page (redirect) integration guide

In your checkout confirmation page, submit the HTML form to the following URL.

Test

```
<form id="kblPaymentForm" action="https://test-ipg.kinabank.com.pg/cgi-bin/cgi_link"
method="POST">
```

Production

```
<form id="kblPaymentForm" action="https://ipg.kinabank.com.pg/cgi-bin/cgi_link" method="POST">
```

Digital Signature

To safeguards against man-in-the-middle attacks, it's mandatory to implement digital signatures for all request and response message.

Digital signature is a mathematical scheme to verify the authenticity of message exchanged between two nodes. A valid digital signature lets a recipient know the message was created by a known sender, and that it was not altered while transmitting.

Kina Payment Gateway employs Hash-based Message Authentication Code (HMAC) as a form of digital signature. HMAC involves the use a cryptographic key (secret key) in conjunction with a hash function

Secret key

A secret key is used to generate/verify the HMAC.

For integration test, use the secret key defined in Test Data section of this document. Please liaise with your bank representative to obtain secret key for production live system.

Merchant must take extra precautions to safeguard the production secret key. Do not expose the secret key in any frontend webpage.

MAC source string

The fields used to generate digital signatures are defined in the following table

TRTYPE	MAC Fields for Request	MAC Fields for Response
1 – Retail Financial Request	TERMINAL TRTYPE AMOUNT CURRENCY ORDER MERCHANT EMAIL BACKREF TIMESTAMP MERCH_NAME COUNTRY MERCH_URL MERCH_GMT DESC NONCE	ACTION RC APPROVAL CURRENCY AMOUNT *Please format the returned amount with decimal point (2 decimal point) TERMINAL TRTYPE ORDER RRN MERCHANT TIMESTAMP INT_REF NONCE
24 – Reversal Request	ORDER	ORDER
90 – Check Transaction Status	ORDER	ORDER

Digital Signature in Request

To generate a digital signature, merchant system must assemble a MAC source string according to the above tables. All field values are prefixed with the decimal field length in ASCII and concatenated in exact same order defined in the above table. If the field is not present, the '-' character is added to the message in its place.

Suppose we have a transaction of following values

Field	Length	Value
TERMINAL	8	99999999
TRTYPE	1	1
AMOUNT	5	11.48
CURRENCY	3	USD
ORDER	6	771446
MERCHANT	15	123456789012345
EMAIL	19	pgw@mail.sample.com
BACKREF	33	https://www.sample.com/shop/reply
TIMESTAMP	14	20030105153021
MERCH_NAME	17	Books Online Inc.
COUNTRY	0	
MERCH_URL	14	www.sample.com
MERCH_GMT	0	
DESC	16	IT Books. Qty: 2
NONCE	16	F2B2DD7E603A7ADA

MAC source string for the above example:

899999999115 11.48 3USD6 771446 15 123456789012345 19 pgw@mail.sample.com 33 https://www.sample.com/shop/reply 14 20030105153021 17 Books Online Inc. -14 www.sample.com -16 IT Books. Qty: 2 16 F2B2DD7E603A7ADA

After the MAC source string is assembled, the merchant system must apply a cryptographic algorithm to generate the message authentication code. The default algorithm is **HMAC_SHA256**.

Below is an example of **HMAC_SHA256** implementation using JS.

JavaScript Examples

```
let macSourceString =
'89999999911511.483USD6771446151234567890123451 9pgw@mail.sample.com33https://www.sample.com
/shop/reply142003010515302117Books Online Inc.-14www.sample.com-16IT Books. Qty:
216F2B2DD7E603A7ADA';

const secret = 'debdd135e436905c7a02f20c56c83a4c501adf555457f0df';
let txtKey = CryptoJS.enc.Hex.parse(secret);
let encryptedMac = CryptoJS.HmacSHA256(macSourceString, txtKey);
```

Generation of digital signature should only be done in a secured backend system and the MAC result can be stored in the “P_SIGN” hidden field in the order confirmation page

Digital Signature in Response

Digital signature is stored in “P_SIGN” field in response message.

To verify the authenticity of the response message. Merchant’s system must compute a digital signature by employing the same method described above.

1. First assemble the MAC source string from the response.
2. Apply HMAC_SHA256 algorithm and compare the result with the P_SIGN values returned by payment gateway.

EGW Response Code

RC	Description
-1	A mandatory request field is not filled in
-2	CGI request validation failed
-3	Acquirer host (NS) does not respond or wrong format of e-gateway response template file
-4	No connection to the acquirer host (NS)
-5	The acquirer host (NS) connection failed during transaction processing
-6	e-Gateway configuration error
-7	The acquirer host (NS) response is invalid, e.g. mandatory fields missing
-8	Error in the "Card number" request field
-9	Error in the "Card expiration date" request field
-10	Error in the "Amount" request field
-11	Error in the "Currency" request field
-12	Error in the "Merchant ID" request field
-13	The referrer IP address (usually the merchant's IP) is not the one expected
-14	No connection to the iPOS PINpad or agent program is not running on the iPOS computer/workstation
-15	Error in the "RRN" request field
-16	Another transaction is being performed on the terminal
-17	The terminal is denied access to the e-Gateway
-18	Error in the CVC2 or CVC2 Description request fields
-19	Error in the authentication information request or authentication failed.
-20	A permitted time interval (1 hour by default) between the transaction Time Stamp request field and the e-Gateway time is exceeded
-21	The transaction has already been executed
-22	Transaction contains invalid authentication information
-23	Invalid transaction context
-24	Transaction context data mismatch
-25	Transaction canceled (e.g. by user)
-26	Invalid action BIN
-27	Invalid merchant name
-28	Invalid incoming addendum(s)
-29	Invalid/duplicate authentication reference
-30	Transaction was declined as fraud
-31	Transaction already in progress
-32	Duplicate declined transaction
-33	Client authentication by random amount or verify one-time code in progress
-34	MasterCard Installment client choice in progress
-35	MasterCard Installments auto canceled
-96	Mandatory fields are missing
-97	Session Timeout / Not Login
-98	Exceed OTP attempts limit
-99	Transaction aborted due to browser refresh

Test Data

Following test data can be used to perform integration testing with KINA PAYMENT GATEWAY in test environment.

Test Card

Card Type	Card Attributes
Visa Card	4012000000003010 Expiry: 12/27 or any future date CVV: 123
Kina Debit Card	5076480200021147 Expiry: 03/24

Test Merchant for iframe

Field	Value
TERMINAL	99999001
MERCHANT	000000099999001

Test Merchant for Hosted Payment Page

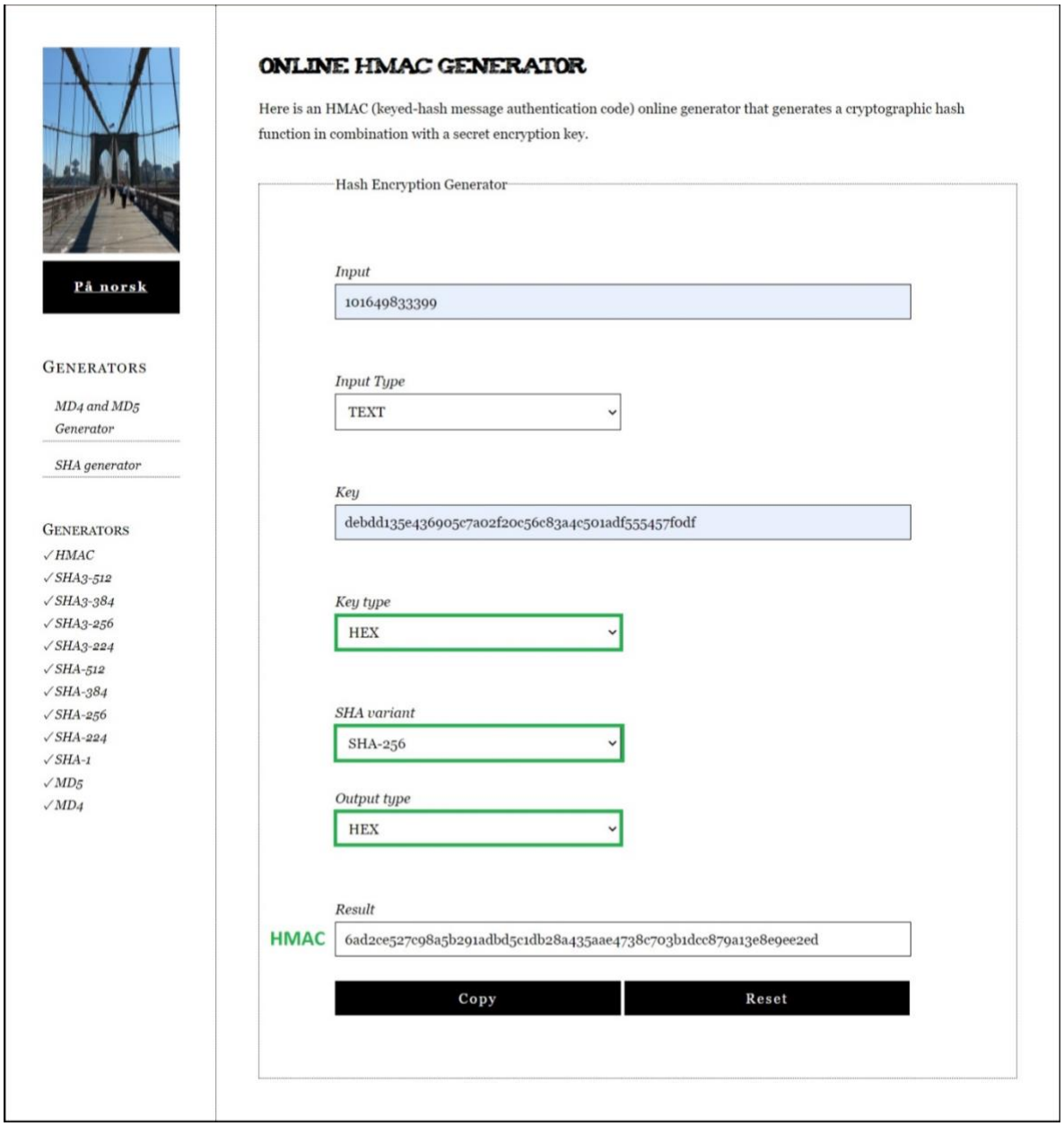
Field	Value
TERMINAL	99999004
MERCHANT	000000099999004

Secret Key

debdd135e436905c7a02f20c56c83a4c501adf555457f0df

"Please ensure Secret Key data type is set to HEX"

Online HMAC Calculator

A good reference site for HMAC testing.

https://www.liavaag.org/English/SHA-Generator/HMAC/